NAJWYŻSZA IZBA KONTROLI

DELEGATURA WE WROCŁAWIU

LWR.410.13.6.2024

**Pan**
**Tomasz Frischmann**
**Burmistrz Miasta Oława**
Urząd Miejski w Oławie
Plac Zamkowy 15
55-200 Oława

# WYSTĄPIENIE POKONTROLNE

P/24/004 – „Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego”

# I. Dane identyfikacyjne

| | |
|---|---|
| Jednostka kontrolowana | Urząd Miejski w Oławie[1], Plac Zamkowy 15, 55-200 Oława. |
| Kierownik jednostki kontrolowanej | Tomasz Frischmann, Burmistrz Miasta Oława[2] od 9 grudnia 2014 r. |
| Zakres przedmiotowy kontroli | Rozwiązania organizacyjne i techniczne w zakresie zapewnienia bezpieczeństwa przetwarzania informacji oraz zapewnienia ciągłości działania w Urzędzie i ich stosowanie. |
| Okres objęty kontrolą | Od 1 stycznia 2023 r. do dnia zakończenia kontroli w 2024 r.[3] (także okresy wcześniejsze w zakresie uczestnictwa w programie Cyfrowa Gmina). |
| Podstawa prawna podjęcia kontroli | Artykuł 2 ust. 2 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]. |
| Jednostka przeprowadzająca kontrolę | Najwyższa Izba Kontroli<br>Delegatura we Wrocławiu |
| Kontrolerzy | 1. Cezary Mazik, główny specjalista kontroli państwowej, upoważnienie do kontroli nr LWR/96/2024 z 26 czerwca 2024 r.<br>2. Radosław Chodziński, starszy inspektor kontroli państwowej, upoważnienie do kontroli nr LWR/106/2024 z 18 lipca 2024 r. |

(akta kontroli: str. 1-2, 5)

[1] Dalej: UM w Oławie lub Urząd.
[2] Dalej: Burmistrz.
[3] 6 września 2024 r.
[4] Dz. U. z 2022 r. poz. 623. Dalej: ustawa o NIK.

# II. Ocena ogólna[5] kontrolowanej działalności

**OCENA OGÓLNA**

Urząd nie zawsze prawidłowo i rzetelnie realizował zadania związane z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

W okresie objętym kontrolą opracowano i wdrożono System Zarządzania Bezpieczeństwem Informacji[6], o którym mowa w § 19 ust. 1 rozporządzenia Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[7]. Sporządzono także dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/679 z 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)[8].

Prawidłowo zidentyfikowano również zbiory danych podlegających zabezpieczeniu. Wyznaczono pracowników odpowiedzialnych za bezpieczeństwo informacji, zapewnienie ciągłości działania, ochronę danych osobowych oraz za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Utrzymywano aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. Wprowadzono rozwiązania zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, a uprawnienia pracowników w systemach informatycznych nie wykraczały poza zakres określony w ich zakresach obowiązków. Wprowadzono prawidłowe zabezpieczenia techniczne w systemach informatycznych w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem. Ustanowiono zasady (procedury) gwarantujące bezpieczną pracę przy pracy zdalnej, w szczególności przy przetwarzaniu mobilnym i pracy na odległość. Przeprowadzono także szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji oraz zapewniono przeprowadzenie audytu z zakresu bezpieczeństwa informacji.

W trakcie kontroli stwierdzono jednak szereg nieprawidłowości polegających w szczególności na: **[1]** nie w pełni rzetelnych analizach ryzyka w związku z potrzebą zachowania ciągłości działania systemów IT, **[2]** nieopracowaniu i niewdrożeniu kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych, **[3]** niepoddawaniu w okresie objętym kontrolą przeglądowi i aktualizacji dokumentacji SZBI, **[4]** braku kart uprawnień do systemów informatycznych dla trzech pracowników, **[5]** nieodebraniu dwóm osobom, które zakończyły pracę w Urzędzie, uprawnień do poczty służbowej, **[6]** niewłaściwym zabezpieczeniu pomieszczenia serwerowni, **[7]** braku zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji w dwóch umowach serwisowych oraz **[8]** nie w pełni rzetelnych analizach ryzyka.

[5] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.
[6] Dalej: SZBI.
[7] Dz. U. poz. 773. Dalej: rozporządzenie KRI.
[8] Dz.Urz.UE.L 119 z 04.05.2016, str. 1, ze zm. Dalej: RODO.

# III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

## 1. Organizacja bezpieczeństwa informacji i zapewnienia ciągłości działania systemów informatycznych

Opis stanu faktycznego

**1.1.** W UM w Oławie zidentyfikowano 160 zbiorów danych, które są w nim przetwarzane i podlegają zabezpieczeniu. Dotyczyły one m.in. rozpatrywania skarg, wniosków i petycji; prowadzenia wyborów ławników sądowych; wyborów do młodzieżowej rady gminy; nadzoru nad spółkami komunalnymi; danych władających nieruchomościami; kwalifikacji wojskowej; realizacji zadań obronnych; rekrutacji pracowników Urzędu; przyznania Karty Dużej Rodziny; wydawania decyzji o warunkach zabudowy; prowadzenia rejestru mieszkańców i rejestru PESEL; poboru podatków i opłat lokalnych; rejestracji stanu cywilnego i innych.

Zidentyfikowanym zbiorom danych przypisano odpowiedni poziom ochrony, zgodny z ich wagą. Wśród technicznych i organizacyjnych środków bezpieczeństwa wyróżniano m.in.: kontrolę dostępu do systemu informatycznego; dostęp do pomieszczeń tylko dla upoważnionych osób; zabezpieczenie komputerów przed możliwością użytkowania przez osoby nieuprawnione; przechowywanie dokumentów w szafach zamykanych na klucz; przetwarzanie danych przez osoby posiadające upoważnienie.

(akta kontroli: str. 307, 370-390)

**1.2.** W Urzędzie opracowano i wdrożono SZBI, o którym mowa w § 19 ust. 1 rozporządzenia KRI.

Składał się on przede wszystkim z Polityki Bezpieczeństwa Informacji UM w Oławie[10] (zawierającej Politykę Ochrony Danych Osobowych[11], Instrukcję Zarządzania Systemem Informatycznym[12] oraz Instrukcję Korzystania z Systemu Informatycznego). Innymi dokumentami tworzącymi SZBI były: Regulamin pracy zdalnej[13]; Procedura nadawania i odbierania upoważnień do przetwarzania danych osobowych i przebywania w pomieszczeniach, w których dochodzi do przetwarzania danych osobowych[14]; Procedura postępowania w sytuacji naruszenia ochrony danych osobowych, lub podejrzenia naruszenia danych osobowych[15]; Procedura zawierania i prowadzenia rejestru umów powierzenia przetwarzania danych osobowych w UM w Oławie[16]; Procedura postępowania z kluczami oraz zabezpieczenia budynków Urzędu[17]. Dokumenty te zostały zatwierdzone przez Burmistrza oraz zakomunikowane pracownikom Urzędu. Komórką właściwą za opracowanie i wdrożenie dokumentacji SZBI był Wydział Informatyki Urzędu[18] oraz Inspektor Ochrony Danych Urzędu[19] (w zakresie ochrony danych osobowych).
Wyżej wymieniona dokumentacja w dużym stopniu ukierunkowana była na ochronę danych osobowych, lecz ze względu na powołanie się i uregulowanie niektórych zagadnień wynikających z rozporządzenia KRI spełniała także wymogi SZBI.

---

[9] Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.
[10] Wprowadzona zarządzeniem Burmistrza nr 2/120/2016 z 8 stycznia 2016 r., zmieniona zarządzeniem Burmistrza nr 8/120/2022 z 23 marca 2022 r. Dalej: PBI.
[11] Dalej: PODO.
[12] Dalej: IZSI.
[13] Wprowadzony zarządzeniem Burmistrza nr 9/120/2020 z 6 kwietnia 2020 r.
[14] Wprowadzona zarządzeniem Burmistrza nr 10/120/2021 z 9 kwietnia 2021 r.
[15] Wprowadzona zarządzeniem Burmistrza nr 11/120/2022 z 7 kwietnia 2022 r.
[16] Wprowadzona zarządzeniem Burmistrza nr 12/120/2022 z 7 kwietnia 2022 r.
[17] Wprowadzona zarządzeniem Burmistrza nr 18/120/2024 z 22 lipca 2024 r.
[18] Dalej: Wydział IT.
[19] Dalej: IOD.

W Urzędzie opracowano dodatkowo procedurę dotyczącą: [1] zabezpieczenia dokumentów przed wysłaniem drogą elektroniczną za pomocą 7-zip oraz [2] drukowania dokumentów przesyłanych do drukarki w innym pomieszczeniu. Zostały one zakomunikowane pracownikom Urzędu.

(akta kontroli: str. 91-225, 307, 310-315)

**1.3.** W UM w Oławie sporządzono dokumentację w zakresie ochrony danych osobowych uwzględniającą wymogi RODO. Była ona częścią SZBI (o czym mowa w punkcie 1.2 wystąpienia pokontrolnego). Jeden z głównych elementów tej dokumentacji, PODO zawierała m.in. wykaz budynków i pomieszczeń, w których są przetwarzane dane osobowe, strukturę zbiorów danych osobowych, sposób przepływu danych osobowych pomiędzy systemami, środki techniczne i organizacyjne niezbędne dla zapewnienia poufności, integralności i rozliczalności przetwarzanych danych osobowych. Ponadto wprowadzono procedury nadawania i odbierania upoważnień do przetwarzania danych osobowych, procedury postępowania w sytuacji naruszenia ochrony danych osobowych, procedury zawierania i prowadzenia rejestru umów powierzenia przetwarzania danych osobowych i inne. Dokumentacja ta została zatwierdzona przez Burmistrza i zakomunikowana odpowiedzialnym pracownikom Urzędu.

(akta kontroli: str. 137-225)

**1.4.** W okresie objętym kontrolą w Urzędzie prowadzone były coroczne analizy ryzyka w związku z potrzebą zachowania ciągłości działania systemów informatycznych. Dokumentowano je w rejestrze ryzyka na dany rok. Rejestr ten składał się z trzech głównych elementów: [1] identyfikacji ryzyka, [2] analizy ryzyka, [3] odpowiedzi na ryzyko. Analizy te nie były jednak w pełni rzetelne, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 320-327)

**1.5.** Zasady polityki ciągłości działania Urzędu zostały ujęte w IZSI. Opisano tam środki i metody stosowane w zarządzaniu oraz eksploatacji systemów informatycznych w celu ich odpowiedniego zabezpieczenia i zapewnienia ciągłości działania. W dokumencie tym przedstawiono również m.in. zasady: bezpieczeństwa fizycznego, zgłaszania incydentów, zarządzania sprzętem informatycznym, tworzenia kopii zapasowych, zarządzania bezpieczeństwem sieciowym, zarządzania oprogramowaniem. Zasady te zostały zakomunikowane pracownikom w ramach zakomunikowania dokumentacji SZBI.

(akta kontroli: str. 138-172)

**1.6.** W Urzędzie nie opracowano i nie wdrożono kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

Należy nadmienić, że w dokumentacji SZBI określono ważne dla zapewnienia ciągłości działania zasady dotyczące m.in. wykonywania kopii zapasowych. Nie przyjęły one jednak formy kompletnego planu w wyżej wymienionym zakresie.

Czas przywrócenia ciągłości działania systemów informatycznych Urzędu, omówiono w punkcie 2.14 wystąpienia pokontrolnego.

(akta kontroli: str. 137-225, 308)

**1.7.** Pomimo faktu, że w Urzędzie nie opracowano i nie wdrożono kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych, to według wyjaśnień Zastępcy Burmistrza, *każdy wdrożony mechanizm służący zachowaniu ciągłości działania i możliwości odtworzenia był testowany w trakcie wdrożenia. Ponadto newralgiczne systemy były dodatkowo testowane okresowo. PBI UM w Oławie*

*nie wymaga formalnego dokumentowania testowania i trenowania planów ciągłości i odtwarzania*.

NIK wskazuje, że zgodnie z normą ISO 22301 *w przypadku planu zapewnienia ciągłości działania oraz planów odtworzeniowych istotne jest ich cykliczne testowanie w celu uzyskania potwierdzenia, że w sytuacji wystąpienia incydentu ciągłości działania zadziałają one prawidłowo. Nie jest możliwe zasymulowanie w pełni zaistniałej katastrofy, np. zalanie, pożar budynku, dlatego też plany te powinny być testowane jedynie w możliwym zakresie. Istotne jest zidentyfikowanie słabych punktów tych planów w trakcie ćwiczeń. W ćwiczeniach tych powinni brać udział wszyscy zaangażowani w daną działalność pracownicy. Wszystkie działania w tym zakresie winny być dokumentowane.*

(akta kontroli: str. 308)

**1.8.** Dokumentacja SZBI Urzędu, w okresie objętym kontrolą, nie była poddawana formalnemu przeglądowi i aktualizacji[20], czym naruszono § 19 ust. 2 pkt 1 rozporządzenia KRI. Powyższe opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 308)

**1.9.** W Urzędzie zostali wyznaczeni pracownicy odpowiedzialni za bezpieczeństwo informacji oraz zapewnienie ciągłości działania. Byli to trzej pracownicy Wydziału IT oraz osoba pełniąca funkcję IOD

Pracownikom Wydziału IT w zakresach obowiązków przypisano m.in. następujące obowiązki: zapewnienie bezpieczeństwa informatycznego; zapewnienie ciągłości działania systemów teleinformatycznych Urzędu; administrowanie serwerami i systemami informatycznymi Urzędu; tworzenie kopii zapasowych systemów teleinformatycznych i programów umożliwiających odtworzenie danych w przypadku awarii; nadzór nad bezpieczeństwem systemu teleinformatycznego i zabezpieczenie danych przed ich zniszczeniem, uszkodzeniem lub niepożądanym dostępem; nadzór przestrzegania procedur związanych z bezpieczeństwem informatycznym.

Z kolei z zakresu czynności IOD wynikało m.in.: prowadzenie lub organizowanie szkoleń dla pracowników Urzędu z zakresu bezpieczeństwa informacji.

Pracownicy Wydziału IT posiadali odpowiednie kwalifikacje do pełnienia tej funkcji, potwierdzone wykształceniem, szkoleniami oraz praktyką zawodową.

(akta kontroli: str. 308-309, 332-346)

**1.10.** Zgodnie z art. 37 ust. 1 i 5 RODO oraz art. 8 ustawy z dnia 10 maja 2018 r. o ochronie danych osobowych[21] w Urzędzie wyznaczono osobę na stanowisko IOD[22].

W zakresie obowiązków osoby pełniącej funkcję IOD ustalono m.in. monitorowanie przestrzegania przepisów o ochronie danych osobowych; informowanie administratora, podmiotów przetwarzających oraz pracowników, którzy przetwarzają dane osobowe, o obowiązkach wynikających z przepisów o ochronie danych osobowych, doradzanie im w tej sprawie i rekomendowanie określonych działań; opracowywanie polityk i procedur z zakresu ochrony danych osobowych; zbieranie informacji w celu identyfikacji procesów przetwarzania; podnoszenie świadomości osób przetwarzających dane osobowe; współpraca z organem nadzorczym oraz pełnienie funkcji punktu kontaktowego pomiędzy administratorem a Urzędem Ochrony Danych Osobowych.

[20] Za wyjątkiem wprowadzenia (22 lipca 2024 r.) Procedury postępowania z kluczami oraz zabezpieczenia budynków Urzędu.
[21] Dz. U. z 2019 r. poz. 1781.
[22] Wyznaczona zarządzeniem Burmistrza Nr 14/120/2020 z 14 kwietnia 2020 r.

Osoba ta posiadała odpowiednie kwalifikacje do pełnienia tej funkcji, potwierdzone szkoleniami oraz praktyką zawodową.

(akta kontroli: str. 10-15, 391-393)

**1.11.** Funkcję IOD w Urzędzie pełnił Naczelnik Wydziału Zarządzania Kryzysowego, Spraw Obronnych i Bezpieczeństwa Informacji, podlegający bezpośrednio Burmistrzowi[23]. W kontekście konfliktu interesów Burmistrz wyjaśnił, m.in., że *zgodnie z art. 38 ust. 6 RODO, IOD może wykonywać inne zadania i obowiązki. Zadania Naczelnika ww. Wydziału nie powodują konfliktu interesów z funkcją IOD. Oba stanowiska są różnorodne i niezależne. IOD nie uczestniczy w decyzjach operacyjnych związanych z przetwarzaniem danych osobowych w ramach powyższego Wydziału. Naczelnik Wydziału Zarządzania Kryzysowego, Spraw Obronnych i Bezpieczeństwa Informacji Urzędu, nie określał sposobów i celów przetwarzania danych osobowych. Sprawami tymi zajmował się inny pracownik tego Wydziału. Ponadto mechanizm identyfikujący powstanie konfliktu interesów i zastosowanie w związku z tym środków zaradczych, tworzą przepisy zarządzenia Burmistrza[24] w sprawie ustalenia zasad funkcjonowania kontroli zarządczej w Gminie Miasto Oława*.

(akta kontroli: str. 5, 8, 10, 13-15, 16-60, 309, 404-406, 442, 470, 477)

**1.12.** Burmistrz[25], zgodnie z art. 21 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[26], wyznaczył osobę odpowiedzialną w Urzędzie za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa[27]. Dane tej osoby, obejmujące imię i nazwisko, numer telefonu oraz adres poczty elektronicznej, zostały przekazane do CSIRT NASK[28], 29 czerwca 2021 r., a więc 117 dni po upływie 14 dniowego terminu na tę czynność przewidzianego w art. 22 ust. 1 pkt 5 ustawy o ksc, co szczegółowo opisano w sekcji *Stwierdzone nieprawidłowości*.

Nie skorzystano natomiast z uprawnienia określonego w art. 21 ust. 2 i 3 ustawy o ksc, tj. nie wyznaczono jednej osoby odpowiedzialnej za utrzymywanie ww. kontaktów w zakresie zadań publicznych zależnych od systemów informacyjnych, realizowanych przez jednostki organizacyjne Urzędu oraz jednostki podległe i nadzorowane przez Burmistrza. Jak wyjaśnił, wynikało to z tego, *że każdy kierownik jednostki ponosi odpowiedzialność za całokształt spraw wchodzących w zakres jej działalności*.

(akta kontroli: str. 407, 421-424)

**1.13.** PBI Urzędu nie wymagała sporządzenia dodatkowych dokumentów wykonawczych.

(akta kontroli: str. 137-183, 407-408)

**1.14.** Zgodnie z § 19 ust. 2 pkt 2 rozporządzenia KRI, w Urzędzie utrzymywano aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację. W tym celu Urząd korzystał ze specjalistycznego oprogramowania, które pozwalało m.in. na inwentaryzowanie oprogramowania i sprzętu oraz raportowanie wydajności zasobów sieciowych. Przeprowadzone oględziny[29] na próbie celowej 10 komputerów, jednego serwera, dwóch laptopów, jednego routera i jednej drukarki wykazały, że powyższy system

[23] Zgodnie z Regulaminem Organizacyjnym Urzędu, którego tekst jednolity wprowadzono zarządzeniem Burmistrza nr 6/120/2024 z 1 marca 2024 r.
[24] Nr 4/120/2023 z 1 marca 2023 r.
[25] Zarządzeniem nr 6/120/2021 z 18 lutego 2021 r.
[26] Dz. U. z 2024 r. poz. 1077. Dalej: ustawa o ksc.
[27] Osobą wyznaczoną był Naczelnik Wydziału IT.
[28] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy.
[29] 26 lipca 2024 r.

zawierał dane m.in. w zakresie zainstalowanego oprogramowania, sprzętu, konfiguracji systemu oraz osoby odpowiedzialnej za sprzęt (użytkownika).

(akta kontroli: str. 394)

**1.15.** Urząd przystąpił do Programu „Cyberbezpieczny Samorząd”[30], realizowanego przez Centrum Projektów Polska Cyfrowa w ramach Funduszy Europejskich na Rozwój Cyfrowy 2021-2027. Umowa o powierzenie grantu[31] o wartości 855,0 tys. zł[32], została zawarta 8 kwietnia 2024 r.[33], a czas jej realizacji ustalono na maksymalnie 24 miesiące od dnia jej wejścia w życie. W ramach tej umowy zaplanowano: [1] opracowanie nowej dokumentacji SZBI oraz przeprowadzenie audytu SZBI; [2] zakup, wdrożenie i utrzymanie sprzętu komputerowego oraz oprogramowania w celu podniesienia poziomu cyberbezpieczeństwa, w tym zakup urządzeń UTM[34], przełączników sieciowych, oprogramowania klasy NAC[35], oprogramowania do centralnego zarządzania i monitorowania sprzętem komputerowym, oprogramowania, serwera i dysków do backupu; [3] przeprowadzenie szkoleń w zakresie wymagań SZBI i cyberbezpieczeństwa dla pracowników Urzędu.

Jako element pomiaru poprawy cyberbezpieczeństwa w wyniku realizacji tego Programu przewidziano ewaluację według kryteriów „Ankiety Dojrzałości Cyberbezpieczeństwa w Jednostce Samorządu Terytorialnego”. Przed rozpoczęciem Programu wypełniono ankietę, w której określono stan obecny w zakresie ośmiu obszarów cyberbezpieczeństwa[36] oraz planowane zmiany w związku z jego realizacją. Ponadto zostanie przeprowadzony audyt wdrożonego – w ramach Programu – nowego SZBI.

(akta kontroli: str. 255-306, 408)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

**1.** Prowadzone w Urzędzie w okresie objętym kontrolą udokumentowane analizy ryzyka zawierające elementy związane z potrzebą zachowania ciągłości działania systemów informatycznych nie były w pełni rzetelne. Agregowały one bowiem poszczególne ryzyka systemów informatycznych wyłącznie w jednej grupie, przypisując im jeden poziom istotności ryzyka oraz identyczne mechanizmy kontroli.

Burmistrz wyjaśnił, że *SZBI Urzędu nie określa zasad zarządzania ryzykiem, dlatego formalna analiza ryzyka prowadzona jest w ramach kontroli zarządczej*. *Dodał również, że procedura analizy ryzyka zostanie opisana w powstającej dokumentacji SZBI*.

NIK wskazuje, że analiza ryzyka w związku z potrzebą zachowania ciągłości działania powinna zidentyfikować i określić ryzyka wraz z dokonaniem ich podziału na zewnętrze oraz wewnętrze. Następnie wskazane jest, aby nadawać tym ryzykom odpowiedni poziom prawdopodobieństwa oraz opisać działania

---

[30] Dalej: Program.

[31] Nr FERC.02.02-CS.01-001/23/1389/ FERC.02.02-CS.01-001/23/2024.

[32] W tym 786,6 tys. zł (dofinansowanie) i 68,4 tys. zł (wkład własny). Na kwotę dofinansowania składały się: 660,7 tys. zł (wkład Unii Europejskiej) i 125,9 tys. zł (wkład budżetu państwa).

[33] Data wejścia w życie przedmiotowej umowy.

[34] Urządzenie UTM (ang. Unified Threat Management), to urządzenia sieciowe, odpowiadające za kompleksową ochronę, nadzorowanie ruchu w sieci lokalnej oraz styk / dostęp do Internetu. Zamiast wielu rozwiązań typu: zapory sieciowe, IPS, filtry antyspamowe, routery itp. - jest jedno rozwiązanie, łączące wszystkie te funkcje.

[35] Ang. Network Access Control – rozwiązanie zapewniające kontrolę dostępu do sieci przez weryfikację bezpieczeństwa i uprawnień urządzenia końcowego, ubiegającego się o dostęp do sieci, uwierzytelnienie stacji lub użytkownika, warunkowe przydzielenie dostępu do określonej sieci.

[36] Były to [1] Zarządzanie, [2] SZBI, [3] Ochrona, [4] Zdarzenia i Monitoring, [5] Reagowanie, [6] Odtwarzanie, [7] Infrastruktura i [8] Telekomunikacja.

obejmujące mechanizmy reagowania na zakłócenia. Analiza taka powinna być także na bieżąco aktualizowana, szczególnie w zakresie ryzyk i działań zapewniających ciągłość działania organizacji.

(akta kontroli: str. 320-327, 428, 515)

**2.** W Urzędzie nie opracowano i nie wdrożono kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych (za wyjątkiem jego niektórych elementów określonych w dokumentacji SZBI, m.in. dotyczących wykonywania kopii zapasowych).

Burmistrz wyjaśnił m.in., że *PBI Urzędu nie zawiera osobnego dokumentu ani rozdziału dotyczącego zapewnienia ciągłości działania oraz planów odtworzeniowych. Zagadnienia z tym związane poruszane są w IZSI. W praktyce, działania podejmowane w zakresie zapewnienia dostępności systemów informatycznych Urzędu, dążą do jak najkrótszego czasu na przywrócenie ciągłości działania.*

NIK wskazuje, że plan ciągłości działania powinien w szczególności dotyczyć tak ważnych zagadnień jak: typologia sieci, klastry i macierze dyskowe, systemowe serwery wirtualne, urządzenia brzegowe.

(akta kontroli: str. 91-225, 429, 444)

**3.** W okresie objętym kontrolą dokumentacja SZBI Urzędu nie była poddawana przeglądowi i aktualizacji[37], co było niezgodne § 19 ust. 2 pkt 1 rozporządzenia KRI.

Według wyjaśnień Zastępcy Burmistrza, *dokumentacja SZBI Urzędu nie była poddawana formalnemu przeglądowi i aktualizacji. Niemniej jednak jest ona poddawana monitorowaniu przez osoby odpowiedzialne za bezpieczeństwo informacji i w miarę potrzeb aktualizowana*.

NIK zauważa, że przeprowadzanie okresowego (nie rzadziej niż raz na 12 miesięcy) przeglądu dokumentacji SZBI, pozwalałoby na dostosowywanie jej do zmieniającego się otoczenia. Brak prowadzenia takiego monitoringu w Urzędzie potwierdza m.in.: powoływanie się w IZSI (w § 7 ust. 1 pkt 2) na ustawę z 29 sierpnia 1997 r. o ochronie danych osobowych[38] (uchylona 25 maja 2018 r.) oraz na nieobowiązujące od 6 lutego 2019 r. rozporządzenie Ministra Spraw Wewnętrznych i Administracji z 29 kwietnia 2004 r. w sprawie dokumentacji przetwarzania danych osobowych oraz warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych[39].

(akta kontroli: str. 308)

**4.** Dane osoby wyznaczonej w dniu 18 lutego 2021 r. (dotychczas) jako odpowiedzialnej w Urzędzie za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa, zostały przekazane do CSIRT NASK w dniu 29 czerwca 2021 r., a więc 117 dni po upływie 14 dniowego terminu na tę czynność przewidzianego w art. 22 ust. 1 pkt 5 ustawy o ksc.

Burmistrz wyjaśnił, iż *przyczyną powyższej nieprawidłowości była błędna interpretacja przepisów ustawy o ksc, w wyniku której 19 lutego 2021 r. wysłano powyższe dane do CSIRT GOV[40] zamiast do CSIRT NASK. Po stwierdzeniu błędu dane te zostały wysłane do właściwego w tych sprawach CSIRT NASK*.

---

[37] Za wyjątkiem wprowadzenia (22 lipca 2024 r.) Procedury postępowania z kluczami oraz zabezpieczenia budynków Urzędu.

[38] Dz.U. z 2016 r. poz. 922, ze zm.

[39] Dz.U. Nr 100, poz. 1024.

[40] Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego.

(akta kontroli: str. 421-423, 442)

**OCENA CZĄSTKOWA**

W badanym okresie stosowano dokumentację składającą się na SZBI i PODO, uwzględniającą wymogi odpowiednio rozporządzenia KRI oraz RODO. Niemniej nie dokonywano bieżącej aktualizacji SZBI wraz ze stwierdzanymi zmianami zachodzącymi w otoczeniu. Wyznaczono przy tym pracowników odpowiedzialnych za bezpieczeństwo informacji, zapewnienie ciągłości działania, ochronę danych osobowych oraz za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa. Utrzymywano także aktualność inwentaryzacji sprzętu i oprogramowania służącego do przetwarzania informacji obejmującej ich rodzaj i konfigurację.

Podejmowane w powyższym zakresie działania nie zawsze były jednak prowadzone w sposób skuteczny, rzetelny i prawidłowy. Stwierdzono bowiem nieprawidłowości, które dotyczyły: nie w pełni rzetelnych analiz ryzyka dotyczących zachowania ciągłości działania systemów informatycznych; nieopracowania i niewdrożenia kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych; niepoddawania w okresie objętym kontrolą formalnemu przeglądowi i aktualizacji dokumentacji SZBI; przekazania do CSIRT NASK z opóźnieniem, danych osoby wyznaczonej jako odpowiedzialnej w Urzędzie za utrzymywanie kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

**OBSZAR**

## 2. Wdrożone i wykorzystywane rozwiązania organizacyjne i techniczne zapewniające bezpieczeństwo informacji oraz ciągłość działania

Opis stanu faktycznego

**2.1.** Przyjęte w Urzędzie rozwiązanie, polegające na nieprzyznawaniu użytkownikom uprawnień administracyjnych do systemu operacyjnego, zapobiegało możliwości instalowania nieautoryzowanego oprogramowania przez pracowników Urzędu na komputerach służbowych. Wykonane w ramach oględzin[41] badanie dziesięciu komputerów (w tym pięciu stacjonarnych i pięciu laptopów) wykazało, że żaden z testowanych użytkowników nie posiadał uprawnień (administracyjnych) do instalacji oprogramowania, co było zgodne z § 19 ust. 2 pkt 4 rozporządzenia KRI.

Według wyjaśnień Burmistrza, *w Urzędzie wykorzystywano 17 smartfonów. Wszystkie wykorzystywane w Urzędzie smartfony posiadały system operacyjny Android, a system ten w standardzie nie pozwala na blokadę instalowania dodatkowych aplikacji przez użytkowników. Pozwala natomiast na instalację aplikacji z zaufanego źródła jak „Sklep Google Play". Urządzenia te były zabezpieczone blokadą ekranu i uruchomionym szyfrowaniem pamięci. Użytkownicy smartfonów byli pouczeni co do zasad bezpiecznego ich używania. Ponadto, przyznane pracownikom smartfony nie były przeznaczone do przetwarzania informacji – nie instalowano na nich aplikacji wykorzystywanych w Urzędzie. UM w Oławie nie dysponował tabletami.*

(akta kontroli: str. 439, 443, 505)

**2.2.** Zgodnie z opisaną w IZSI procedurą nadawania uprawnień w systemach informatycznych, uprawnienia do poszczególnych systemów informatycznych nadawał Administrator Systemów Informatycznych[42] – Naczelnik Wydziału IT. Osobami odpowiedzialnymi za określenie uprawnień do systemów informatycznych byli kierownicy komórek organizacyjnych Urzędu. W przypadku osób zatrudnionych na stanowiskach bezpośrednio podległych Burmistrzowi odpowiedzialny w tym zakresie był IOD. Wypełnioną, stosowną kartę uprawnień, kierownik komórki

[41] Przeprowadzonych 5 sierpnia 2024 r.
[42] Dalej: ASI.

organizacyjnej lub IOD miał kierować do ASI w celu ustawienia odpowiednich uprawnień w systemie. Odpowiedzialny za przechowywanie kart uprawnień był ASI.

Badanie[43] losowo wybranej próby 15 pracowników Urzędu (14,85% ogółu zatrudnionych)[44] wykazało, że uprawnienia tych pracowników w systemach informatycznych nie wykraczały poza zakres określony w ich zakresach obowiązków służbowych. Tym nie mniej stwierdzono brak kart uprawnień do systemów informatycznych (na podstawie których ASI nadaje te uprawnienia) dla trzech pracowników, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 142, 458-459, 466)

W § 1 ust. 5 IZSI, zapisano obowiązek cyklicznego przeprowadzania przeglądów nadanych uprawnień w systemach informatycznych. Zgodnie z § 1 ust. 5 pkt 4 i 5 IZSI, wyniki przeglądu należy przekazać Burmistrzowi do zatwierdzenia. UM w Oławie nie dysponował dokumentem zatwierdzonym przez Burmistrza, zawierającym wyniki wyżej wymienionego przeglądu, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 143, 470, 476)

**2.3.** Badanie[45] na próbie ośmiu osób[46] wykazało, że odebrano im uprawnienia do pracy w systemach informatycznych, za wyjątkiem systemu poczty służbowej, w którym aktywne konta posiadało dwóch z nich, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 460-465)

**2.4.** Oględziny[47] trzech systemów informatycznych[48] i mechanizmu Microsoft Active Directory[49] wykazały, że w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem, działało wymuszanie odpowiedniej liczby znaków w hasłach, ich złożoności i okresu zmiany, zgodnie z postanowieniami IZSI w tym zakresie. Było to zgodne z § 19 ust. 2 pkt 7 lit. c rozporządzenia KRI.

Identyfikatory (loginy) użytkowników w wyżej wskazanych systemach miały formę imienną[50], poza kontami administracyjnymi, użytkowanymi wyłącznie przez informatyków.

(akta kontroli: str. 398)

**2.5.** Oględziny[51] pięciu stanowisk pracy[52], na których realizowano zadania z wykorzystaniem aplikacji do obsługi Systemu Rejestrów Państwowych i do ewidencji ludności wykazały, że monitory usytuowane były w sposób uniemożliwiający wgląd do danych przez osoby nieuprawnione. Powyższe spełniało wymogi § 19 ust. 2 pkt 7 rozporządzenia KRI.

(akta kontroli: str. 439)

**2.6.** W UM w Oławie ustanowiono zasady (procedury) gwarantujące bezpieczną pracę przy pracy zdalnej w szczególności przy przetwarzaniu mobilnym i pracy na odległość w Regulaminie pracy zdalnej[53]. W regulaminie tym ustalono m.in. warunki podjęcia pracy zdalnej, warunki jakie musi spełniać miejsce świadczenia pracy zdalnej, kwestię

[43] Podczas oględzin przeprowadzonych 7 sierpnia 2024 r.
[44] Na łącznie 101 pracowników pracujących w systemach informatycznych.
[45] Podczas oględzin przeprowadzonych 7 sierpnia 2024 r.
[46] Wszyscy którzy zakończyli zatrudnienie w Urzędzie w okresie objętym kontrolą.
[47] Przeprowadzone 30 lipca 2024 r.
[48] Służących odpowiednio do: [1] zarządzania sprawami i korespondencją; [2] zarządzania finansami; [3] naliczania wynagrodzeń.
[49] Umożliwiającego centralne zarządzanie tożsamościami i dostępem użytkowników komputerów.
[50] Konstrukcja loginów pozwalała na prostą identyfikację użytkowników.
[51] Przeprowadzone 5 sierpnia 2024 r.
[52] W Wydziale Spraw Obywatelskich Urzędu.
[53] Wprowadzonym zarządzeniem Burmistrza nr 9/120/2020 z 6 kwietnia 2020 r.

bezpieczeństwa pracy zdalnej (w tym urządzenia służące do pracy zdalnej, zabezpieczenia przekazywanych informacji, zasady korzystania z dokumentów w formie papierowej), działania niedozwolone. Opisano zasady korzystania ze sprzętu informatycznego minimalizujące ryzyka kradzieży informacji, w tym urządzeń mobilnych. Wprowadzono rozwiązania informatyczne zapewniające bezpieczną pracę użytkowników w formie pracy zdalnej. Pracownicy Urzędu zostali zapoznani z powyższym regulaminem[54] i zobowiązani do jego stosowania. Powyższe było zgodne z § 19 ust. 2 pkt 8 rozporządzenia KRI.

(akta kontroli: str. 184-189, 429, 433-435)

**2.7.** Nośniki danych znajdujące się w laptopach były szyfrowane przy użyciu specjalistycznego oprogramowania, a dostęp do systemu był zabezpieczony logowaniem. Dodatkowo na komputerach w Urzędzie zainstalowane było oprogramowanie antywirusowe i włączony firewall. Zabezpieczenia te spełniały dyspozycję § 19 ust. 2 pkt 9 i 11 rozporządzenia KRI.

(akta kontroli: str. 429)

**2.8.** Oględziny serwerowni Urzędu[55] wykazały, że zasadniczo posiada ona szereg zabezpieczeń fizycznych w celu zabezpieczenia informacji w sposób uniemożliwiający nieuprawnionemu jej ujawnienie, modyfikację, usunięcie lub zniszczenie, m.in. zlokalizowano serwerownię w wyodrębnionym pomieszczeniu, wyposażono w odpowiednie drzwi wejściowe, klimatyzację, dedykowaną sieć elektryczną i zapasowe zasilanie. Tym nie mniej stwierdzono także elementy wymagające poprawy lub wyeliminowania, o czym szerzej w sekcji *Stwierdzone nieprawidłowości*.

(akta kontroli: str. 436-437)

**2.9.** W okresie objętym kontrolą obowiązywało 12 umów zawartych przez Urząd z podmiotami zewnętrznymi w sprawie zamówienia usług serwisowych systemów informatycznych. Szczegółowe badanie czterech z nich[56] wykazało, że w dwóch umowach serwisowych[57] nie zawarto zapisów gwarantujących zachowanie odpowiedniego poziom bezpieczeństwa informacji, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości.*

(akta kontroli: str. 478-500, 503)

**2.10.** W sytuacji przekazywania sprzętu IT poza Urząd do serwisu, w możliwych przypadkach dyski były wyjmowane (demontowane) i pozostawiane w Urzędzie, a w pozostałych zerowane i/lub szyfrowane. W sytuacji przekazywania sprzętu IT do likwidacji wyspecjalizowanej firmie, dyski były nadpisywane losowymi danymi przy użyciu specjalnego oprogramowania. W sytuacji zbywania sprzętu IT lub przekazania go do ponownego użycia, dane zgromadzone na dysku twardym były trwale usuwane (poprzez nadpisywanie losowymi danymi przy użyciu specjalnego oprogramowania), a licencjonowane programy odinstalowane.

Urząd opracował przede wszystkim procedurę likwidacji sprzętu IT. Natomiast praktyki stosowane przez służby informatyczne Urzędu w sytuacji zbycia urządzenia

[54] Mailowo i w aplikacji Teams.
[55] Przeprowadzone 1 sierpnia 2024 r.
[56] Umowa nr: [1] L224 z 1 stycznia 2024 r. dotycząca systemu Dom 5; [2] IT.271.34.2023 z 4 października 2023 r. dotycząca m.in. systemu R2PłatnikPro; [3] UA-166-2024 z 4 października 2023 r. dotycząca systemu informatycznego PB_USC; [4] IT.271.32.2023 z 29 września 2023 r. dotycząca m.in. systemu eDokument EZD.JST.
[57] Umowa nr: [1] L224 z 1 stycznia 2024 r. dotycząca systemu Dom 5 i [2] IT.271.34.2023 z 4 października 2023 r. dotycząca m.in. systemu R2PłatnikPro.

komputerowego lub przekazania go do ponownego użycia, uwzględniały zapisy określone w pkt A.11.2.7 normy PN-ISO/IEC 27001:2017[58].

(akta kontroli: str. 153, 443, 471)

**2.11.** Polityka sporządzania kopii zapasowych Urzędu została opisana w IZSI. Określała ona zasady tworzenia kopii zapasowych: dokumentów użytkowników, systemów i programów, baz danych, ustawień urządzeń sieciowych, a także zasady ich przechowywania.

NIK wskazuje, że w polityce sporządzania kopii zapasowych należało określić jak długo powinny być przechowywane kopie zapasowe, a także kto powinien mieć do nich dostęp.

(akta kontroli: str. 154-155)

**2.12.** W toku oględzin[59] ustalono, że kopie zapasowe danych tworzone były automatycznie, zgodnie z zasadami określonymi w IZSI, tj. codziennie (w dniach roboczych) po zakończeniu pracy Urzędu. Łącznie tworzone były trzy kopie, które przechowywane były w dwóch odrębnych, odpowiednio zabezpieczonych lokalizacjach (w pierwszej na serwerze do backupu i na dysku USB) oraz w drugiej (na macierzy dyskowej). Fakt dostępu do kopii był rejestrowany w programie do ich tworzenia.

Przeprowadzony w trakcie oględzin test na odzyskiwanie danych z wybranej kopii zapasowej[60] zakończył się poprawnym przywróceniem danych.

Częstotliwość testowania kopii zapasowych zależała od krytyczności systemu (dla działania Urzędu). Testowania tego dokonywano codziennie w dni robocze (systemy najbardziej krytyczne), a w innych przypadkach m.in. podczas cyklicznych kontroli. Burmistrz wyjaśnił, iż *system kopii zapasowej serwerów zawierających systemy informatyczne posiada mechanizm weryfikacji poprawności wykonania kopii zapasowej i sprawdzania jej kondycji w celu minimalizowania ryzyka jej uszkodzenia.*

(akta kontroli: str. 154-155, 472-474, 504, 514)

**2.13.** W Urzędzie nie było odrębnej procedury monitorowania pojemności nośników pamięci masowych (dysków twardych), wykorzystywanych w serwerach, poza zapisami w tym zakresie w IZSI (dotyczącymi także obciążenia procesorów, pamięci RAM). Nie stosowano też oprogramowania automatyzującego monitorowanie ww. pojemności. W toku oględzin[61] ustalono, że informatycy prowadzili tzw. ręczne monitorowanie powyższych dysków. Przeprowadzony w trakcie oględzin test zajętości dysków twardych na trzech serwerach wykazał, że zajętość wynosiła odpowiednio: 45%, 45% i 46%.

(akta kontroli: str. 152-153, 399, 429)

**2.14.** Urząd zidentyfikował kluczowe elementy infrastruktury IT, kluczowych usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych. Zgodnie z wiedzą Urzędu, szacowany czas na przywrócenie pojedynczego systemu (procesu do działania) w przypadku jego uszkodzenia (w zależności od złożoności systemu) wynosił od kilkunastu minut do kilku godzin. Natomiast szacowany czas na przywrócenie wszystkich serwerów na których działają systemy informatyczne (wszystkich procesów do działania) wynosił do 24 godzin. Burmistrz wyjaśnił, że *wyżej zakreślony czas wynika z wiedzy, doświadczenia pracowników Wydziału IT i wyników testów przywracania pojedynczych systemów*. Powyższa wiedza była niezbędna dla zapewnienia ciągłości działania Urzędu. Tym nie mniej nie przyjęła ona jednak formy

[58] Technika informatyczna. Techniki bezpieczeństwa. Systemy zarządzania bezpieczeństwem informacji. Wymagania.
[59] Przeprowadzonych 13 sierpnia 2024 r.
[60] Wykonanej 4 kwietnia 2024 r.
[61] Przeprowadzonych 30 lipca 2024 r.

udokumentowanej analizy. Jak wyjaśnił Burmistrz, *stosowne uregulowania w tym zakresie zostaną wprowadzone w nowej dokumentacji SZBI*.

(akta kontroli: str. 504, 507, 511, 514-515)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

**1.** W wyniku badania losowego wybranej próby 15 pracowników Urzędu (14,85%)[62] stwierdzono brak kart uprawnień do systemów informatycznych (na podstawie których ASI nadaje te uprawnienia) dla trzech pracowników, co było niezgodne z § 1 ust. 2 obowiązującej w Urzędzie IZSI.

Burmistrz wyjaśnił, że *ww. pracownicy zostali zatrudnieni przed wejściem w życie, obowiązującej w urzędzie, PBI z 8 stycznia 2016 r., w której wprowadzono procedurę nadawania uprawnień i wzór karty uprawnień. Pracownicy ci otrzymali uprawnienia na podstawie upoważnień do przetwarzania danych osobowych. W tamtym okresie nie była prowadzona ewidencja uprawnień zawierająca daty nadania uprawnień.*

Zdaniem NIK powyższe braki powinny być wyeliminowane w wyniku prowadzenia cyklicznych przeglądów uprawnień do pracy w systemach informatycznych.

(akta kontroli: str. 458-459, 469)

**2.** Urząd nie dokumentował wyników przeglądu uprawnień do systemów informatycznych, podlegających zatwierdzeniu przez Burmistrza, o którym stanowił § 1 ust. 5 pkt 5 IZSI.

Burmistrz wyjaśnił m.in., że *w Urzędzie przegląd uprawnień jest wykonywany na bieżąco przez kierowników komórek organizacyjnych i IOD, np. w sytuacji zmiany zakresu obowiązków lub stanowiska pracy. W przypadku stwierdzenia zmiany zakresu przetwarzanych informacji i/lub zmiany w dostępie do systemów informatycznych nadawane są nowe upoważnienia i/lub uprawnienia do systemów.* Dodał ponadto m.in., iż *w UM w Oławie nie wykonano przeglądu zgodnie z § 1 ust. 5 IZSI, ponieważ przepis ten daje mniejszą skuteczność kontrolną (raz do roku) niż działania stosowane obecnie. Zapisy § 1 ust. 5 IZSI, przy najbliższej zmianie tej procedury zostaną zaktualizowane do stosowanych w Urzędzie rozwiązań w tym zakresie.*

NIK wskazuje, że dopóki zapisy o zatwierdzeniu przez Burmistrza wyników przeglądu uprawnień do systemów informatycznych znajdują się w obowiązującej IZSI, powinny być stosowane. Pozwoliłyby to uniknąć nieprawidłowości dotyczącej brakujących kart uprawnień do systemów informatycznych (o której mowa w punkcie 2.2 wystąpienia pokontrolnego).

(akta kontroli: str. 143, 470, 476)

**3.** W przypadku dwóch osób spośród ośmiu, które zakończyły pracę w Urzędzie w okresie objętym kontrolą, nie odebrano uprawnień (do kont) do poczty służbowej, pomimo że taki fakt odnotowano na kartach uprawnień. W trakcie prowadzenia oględzin Naczelnik Wydziału IT usunął ww. konta. W przypadku jednego pracownika konto to było aktywne 281 dni od ustania jego zatrudnienia, a w przypadku drugiego pracownika było ono aktywne 162 dni od ustania jego zatrudnienia. Powyższe zaniechanie było niezgodne z § 19 ust. 2 pkt 5 rozporządzenia KRI oraz z § 1 ust. 4 pkt 1 obowiązującej w Urzędzie IZSI.

Burmistrz wyjaśnił, iż ww. *pracownikom po zakończeniu umowy zostały wygenerowane losowe hasła do poczty służbowej, co zabezpieczyło ją przed nieautoryzowanym dostępem. Praktyka taka jest stosowana w przypadkach kiedy*

[62] Na łącznie 101 pracowników pracujących w systemach informatycznych.

*dany adres zostaje przekierowany na jakiś czas na inne konto w celu zachowania ciągłości korespondencji i realizacji rozpoczętych zadań*.

NIK wskazuje, że opisana wyżej praktyka nie jest zgodna z § 19 ust. 2 pkt 5 rozporządzenia KRI, który stanowi o bezzwłocznej zmianie uprawnień, w przypadku zmiany zadań osób zaangażowanych w proces przetwarzania informacji oraz z § 1 ust. 4 pkt 1 IZSI, w myśl którego, przy zakończeniu stosunku pracy następuje całkowite odebranie uprawnień. Dla zachowania ciągłości korespondencji i realizacji rozpoczętych zadań można poinformować osoby korespondujące z Urzędem drogą mailową o zmianie pracownika zajmującego się danymi sprawami i jego adresie e-mail.

(akta kontroli: str. 143, 460-464, 469)

**4.** W pomieszczeniu serwerowni stwierdzono stany wymagające poprawy lub wyeliminowania, a dotyczyły one w szczególności: [1] oznaczenia zewnętrznego pomieszczenia napisem „Serwerownia" (ze względów bezpieczeństwa nie jest wskazane aby informacja o lokalizacji tego pomieszczenia była łatwo dostępna dla osób postronnych); [2] braku prowadzenia pełnej ewidencji wejść do pomieszczenia serwerowni (co utrudniało rozliczanie obecności osób w tym pomieszczeniu); [3] przechowywania pudeł kartonowych (co stwarzało ryzyko pożaru). Powyższe było niezgodne z art. 19 ust. 2 pkt 9 rozporządzenia KRI.

Burmistrz wyjaśnił m.in., iż *ww. oznaczenie serwerowni zostało zgodnie z sugestią usunięte. Dostęp do kluczy do serwerowni i do rozbrojenia jej alarmu mają pracownicy Wydziału IT i administrator budynku Urzędu. W systemie alarmowym zapisywany jest rejestr zdarzeń, w którym ewidencjonowane są zdarzenia takie jak rozbrojenie i uzbrojenie alarmu ze wskazaniem użytkownika, który tego dokonał. Ponadto, w serwerowni w pudełkach przechowywane były niezbędne kable, akcesoria, urządzenia i części sprzętu komputerowego. Pudełka znajdowały się w takiej odległości od działających urządzeń elektrycznych, aby zminimalizować ryzyko pożaru. Zgodnie z sugestią pudełka zostały usunięte z serwerowni, a znajdujące się w nich elementy umieszczono w szafie metalowej.*

NIK wskazuje, że ewidencja wejść do serwerowni powinna obejmować obecność wszystkich osób (aby zachować rozliczalność), a nie tylko użytkownika rozbrajającego i uzbrajającego alarm. Osobie takiej mogą towarzyszyć inne, których już powyższy system nie zewidencjonuje.

(akta kontroli: str. 436-437, 442-443)

**5.** Dwie umowy serwisowe[63] (na cztery objęte badaniem), podpisane z podmiotami zewnętrznymi, nie zawierały zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji (tj. zobowiązujących wykonawcę do zachowania tajemnicy informacji do jakich może mieć dostęp w związku z realizowaniem umowy), co było niezgodne z § 19 ust. 2 pkt 10 rozporządzenia KRI.

Burmistrz wyjaśnił m.in., że *brak wymienionych zapisów wynika ze specyfiki przedmiotu danej umowy a także z innych zapisów określających te zasady. Urząd deklaruje, że przy kolejnych umowach zwróci uwagę na wprowadzenie dodatkowych zapisów o zobowiązaniu wykonawcy do zachowania poufności, tj. tajemnicy informacji.* Dodał ponadto, *że podmioty zewnętrzne nie mają dostępu do informacji przetwarzanych w tych systemach.*

NIK wskazuje, że wymóg zawierania w ww. umowach przedmiotowych zapisów określony jest w przepisach prawa, które Urząd zobowiązany jest przestrzegać.

[63] Umowa nr: [1] L224 z 1 stycznia 2024 r. dotycząca systemu Dom 5 i [2] IT.271.34.2023 z 4 października 2023 r. dotycząca m.in. systemu R2PłatnikPro.

Ponadto nie można wykluczyć wystąpienia okoliczności (uwarunkowanych rodzajem błędu w systemie) w których pracownik zewnętrzny w czasie napraw serwisowych i gwarancyjnych będzie musiał mieć dostęp do przetwarzanych w systemach aktywów informacyjnych.

(akta kontroli: str. 478-484, 503)

**OCENA CZĄSTKOWA**

W okresie objętym kontrolą wprowadzono rozwiązania zapobiegające możliwości instalowania nieautoryzowanego oprogramowania, a uprawnienia pracowników w systemach informatycznych nie wykraczały poza zakres określony w ich zakresach obowiązków. Wprowadzono także prawidłowe zabezpieczenia techniczne w systemach informatycznych w celu zapewnienia ochrony przetwarzanych informacji przed nieuprawnionym dostępem. Ustanowiono zasady (procedury) gwarantujące bezpieczną pracę przy pracy zdalnej w szczególności przy przetwarzaniu mobilnym i pracy na odległość. Przeprowadzano także regularne tworzenie kopii zapasowych danych. Urząd miał wiedzę na temat swoich kluczowych elementów infrastruktury IT, kluczowych usług IT oraz ich zabezpieczeń pod kątem wpływu czynników zewnętrznych.

Podejmowane w niniejszym obszarze kontroli działania nie zawsze były jednak skuteczne, rzetelne i prawidłowe. Stwierdzono bowiem nieprawidłowości, które dotyczyły: braku kart uprawnień do systemów informatycznych dla trzech pracowników; niedysponowania dokumentem zawierającym wyniki przeglądu uprawnień do systemów informatycznych o którym mowa w § 1 ust. 5 IZSI; nieodebrania dwóm osobom które zakończyły pracę w Urzędzie w okresie objętym kontrolą, uprawnień (do kont) do poczty służbowej; niewłaściwego zabezpieczenia pomieszczenia serwerowni oraz braku zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji w dwóch umowach serwisowych (na cztery objęte badaniem).

**OBSZAR**

## 3. Działania w celu zapobiegania incydentom bezpieczeństwa informacji

Opis stanu faktycznego

**3.1.** W UM w Oławie w okresie objętym kontrolą prowadzone były analizy ryzyka (udokumentowane), które zawierały elementy dotyczące ryzyka utraty integralności, dostępności lub poufności informacji. Analizy te nie były w pełni rzetelne, co opisano szczegółowo w sekcji *Stwierdzone nieprawidłowości*.

Ponadto, w Urzędzie prowadzono też analizy ryzyka w powyższym zakresie podczas wdrażania nowych systemów informatycznych lub ich elementów, jak również przy każdej znaczącej aktualizacji lub zmianie konfiguracji tych systemów. Te analizy nie były z kolei dokumentowane.

W okresie objętym kontrolą, podejmowano na bieżąco dalsze, stosowne działania związane z wynikami wyżej wymienionych analiz ryzyka (tj. kontrolowano i ograniczano ryzyko).

(akta kontroli: str. 320-327, 505, 507, 516)

**3.2.** W Urzędzie określono zasady bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji (o których stanowi § 19 ust. 2 pkt 13 rozporządzenia KRI), danych osobowych (o których stanowi art. 33 RODO) i cyberbezpieczeństwa (o których stanowi art. 22 ustawy o ksc). Zostali z nimi zapoznani pracownicy Urzędu. Najbardziej szczegółowo ujęto w dokumentacji SZBI, procedurę zgłaszania (m.in. IOD) incydentów dotyczących naruszenia danych osobowych. Incydenty zaliczane do pozostałych ww. kategorii, zgodnie z zasadami należało zgłaszać do Wydziału IT, który je dalej procedował.

Według wyjaśnień Burmistrza, *w okresie objętym kontrolą*[64] *w Urzędzie nie wystąpiły incydenty w zakresie naruszenia bezpieczeństwa informacji, danych osobowych i cyberbezpieczeństwa*.

(akta kontroli: str. 146-147, 172, 181-182, 443-453)

**3.3.** Od 1 stycznia 2023 r. do 14 sierpnia 2024 r. przeszkolono 66 pracowników Urzędu (65,35%)[65] w zakresie bezpieczeństwa danych osobowych i informacji. Były to szkolenia indywidualne (m.in. dla nowo zatrudnionych pracowników). Prowadził je IOD. Powyższe szkolenia wpisywały się w realizację § 19 ust. 2 pkt 6 rozporządzenia KRI. Dotyczyły spraw związanych m.in. z zagrożeniami bezpieczeństwa informacji, stosowaniem środków zapewniających bezpieczeństwo informacji. Burmistrz wyjaśnił, że *ostatnie szkolenia dla wszystkich pracowników, z zakresu bezpieczeństwa informacji, odbyły się w 2020 i w 2021 r. Obecnie Urząd jest w trakcie realizacji projektu Cyberbezpieczny Samorząd, w ramach którego zaplanowane są dla wszystkich jego pracowników, kolejne szkolenia z tego zakresu na IV kwartał 2024 r.*

(akta kontroli: str. 363-369, 470, 476-477)

**3.4**. W grudniu 2023 r. w Urzędzie przeprowadzono audyt z zakresu bezpieczeństwa informacji. W związku ze stwierdzonymi obszarami niezgodności z wymaganiami prawnymi i obszarami wymagającymi poprawy zalecono przede wszystkim:

- określenie zasad i udokumentowanie analizy ryzyka informacji oraz działań podejmowanych w reakcji na ryzyko,
- opisanie w IZSI zasad zbierania dzienników zdarzeń,
- okresowy eksport dzienników zdarzeń kontrolerów domeny, archiwizowanie dzienników zdarzeń w obszarach: application, security, system.

Burmistrz w kwestii realizacji powyższych zaleceń wyjaśnił, iż *zalecenie dotyczące okresowego eksportu dzienników zdarzeń kontrolerów domeny oraz archiwizowania dzienników zdarzeń w obszarach: application, security, system, zostało zrealizowane. Pozostałe zalecenia zostaną wykonane z chwilą wprowadzenia w Urzędzie nowej dokumentacji SZBI, która powstanie w ramach Programu* (o którym mowa w punkcie 1.15 wystąpienia pokontrolnego).

(akta kontroli: str. 62, 226-254, 408)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Prowadzone w Urzędzie, w okresie objętym kontrolą, analizy ryzyka (udokumentowane), zawierające elementy dotyczące ryzyka utraty integralności, dostępności lub poufności informacji, nie były w pełni rzetelne. Agregowały bowiem poszczególne ryzyka systemów informatycznych w jednej grupie, podobnie jak poziom istotności ryzyka, czy mechanizmy kontroli. Rzetelna analiza ryzyka w tym zakresie powinna być prowadzona oddzielnie do danego zagrożenia.

Burmistrz wyjaśnił, że *przyczyną powyższych nieprawidłowości był brak procedury analizy ryzyka w obecnej dokumentacji SZBI. Procedura taka zostanie opisana w nowej dokumentacji SZBI.*

(akta kontroli: str. 320-327, 505, 507, 515)

**OCENA CZĄSTKOWA**

W okresie objętym kontrolą w Urzędzie obowiązywały zasady bezzwłocznego zgłaszania incydentów naruszenia bezpieczeństwa informacji, danych osobowych i cyberbezpieczeństwa. Przeprowadzono także szkolenia dla pracowników zaangażowanych w proces przetwarzania informacji. Zapewniono przeprowadzenie audytu z zakresu bezpieczeństwa informacji. Niemniej, prowadzone

[64] Do 7 sierpnia 2024 r.
[65] Pracujących na systemach informatycznych.

udokumentowane analizy ryzyka, zawierające elementy dotyczące ryzyka utraty integralności, dostępności lub poufności informacji, nie były w pełni rzetelne.

# IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Uwaga

NIK zwraca uwagę, że skala stwierdzonych nieprawidłowości wskazuje na potrzebę wzmocnienia przez Burmistrza działań podejmowanych w obszarze kontroli zarządczej, o której mowa w art. 68 ust. 1 i 2 ustawy z 27 sierpnia 2009 r. o finansach publicznych[66], w celu zapewnienia zgodnego z prawem, terminowego i efektywnego realizowania celów i zadań Urzędu w zakresie związanym z zapewnieniem bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych.

Wnioski

1. Przeprowadzenie pełnej analizy ryzyka uwzględniającego konieczność zachowania ciągłości działania systemów oraz ryzyka utraty integralności, dostępności lub poufności informacji.
2. Opracowanie i wdrożenie kompletnego planu zapewnienia ciągłości działania oraz planów odtworzeniowych.
3. Aktualizowanie dokumentacji składającej się na SZBI w zakresie zmieniającego się otoczenia.
4. Uzupełnienie brakujących kart uprawnień do systemów informatycznych.
5. Przeprowadzanie cyklicznego przeglądu uprawnień do systemów informatycznych oraz przedkładanie jego wyników do zatwierdzenia Burmistrzowi zgodnie z IZSI.
6. Podjęcie działań w celu zapewnienia niezwłocznego i całkowitego odbierania uprawnień do wszystkich systemów informatycznych, osobom posiadającym taki dostęp, które zakończyły stosunek pracy w Urzędzie.
7. Podjęcie działań w celu zapobieżenia występowaniu nieprawidłowości w pomieszczeniu serwerowni w tym w zakresie wprowadzenia rejestru wejść.
8. Zawieranie w umowach serwisowych zapisów gwarantujących zachowanie odpowiedniego poziomu bezpieczeństwa informacji.

[66] Dz. U. z 2023 r. poz. 1270, ze zm.

# V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do dyrektora Delegatury NIK we Wrocławiu. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 dni od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Wrocław, 18 września 2024 r.

Najwyższa Izba Kontroli
Delegatura we Wrocławiu
Dyrektor
z up. p.o. Wicedyrektor
Artur Urban

.....
*podpis*

Kontroler
Cezary Mazik
Główny specjalista kontroli państwowej

.....
*podpis*